QD-SS-011
REVISION D
EFFECTIVE DATE: September 24, 2004

ORGANIZATIONAL INSTRUCTION

PROCEDURES FOR PERFORMING HAZARD ANALYSIS

OPR(s)	**OPR DESIGNEE**
QD10, QD20, QD30, and QD40	**Sherry Jennings**

CHECK THE MASTER LIST AT: http://inside.msfc.nasa.gov/MIDL/
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		3/17/99	
Revision	A	6/9/99	Changes made to reflect new organization code changes and/or Changes made to reflect new directives renumbering scheme and to incorporate the corrective action for closure of NCR 266
Revision	B	11/30/99	Additional changes required to implement RCAR 113 Corrective Actions
Revision	C	9/09/02	Format and numbering change to implement requirements of QS-A-001 rev F.
Revision	D	9/24/04	Revised to bring document in compliance with the HQ Rules Review Action (CAITS: 04-DA01-0387). Changes were also made to reflect S&MA organizational name changes (i.e., QS to QD).

PROCEDURES FOR PERFORMING HAZARD ANALYSIS

1. PURPOSE, SCOPE, APPLICABILITY (As Required)

1.1 Scope. This Organizational Issuance (OI) provides instructions for Safety and Mission Assurance (S&MA) System Safety engineers when developing hazard analyses in support of MSFC projects.

1.2 Purpose. The purpose of this OI is to provide the process and procedures for developing hazard analyses.

1.3 Applicability. The process and procedures documented herein apply to all hazard analyses developed in support of MSFC projects including, but not limited to, Space Shuttle, Space Station, Reusable Launch Vehicles, Expendable Launch Vehicles, and their payloads.

2. DOCUMENTS (Applicable and/or Reference)

2.1. Applicable Documents

MWI 1700.2 D	System Safety Program
QD-A-005.	Professional Development Roadmap (PDRM) for System Safety Engineers
	For Space Shuttle Project Only
NSTS 22254	Methodology for Conduct of Space Shuttle Program Hazard Analyses
	Space Station Only
SSP 30599	Safety Review Process for the International Space Station

2.2. Reference Documents

	For All Projects
NPR 8715.3	NASA Safety Manual
	For Payloads Projects Only
NSTS 1700.7	Safety Policy and Requirements for Payloads Using the Space Transportation System

NSTS 1700.7 (ISS Add.)	Safety Policy and Requirements for Payloads Using the International Space Station
KHB 1700.7	Space Shuttle Payload Ground Safety Handbook
NSTS 13830	Implementation Procedure for NSTS Payloads System Safety Requirements
EWR 127-1	Eastern and Western Range 127-1, Range Safety Requirement, 1997 Edition
	Space Station Only
SSP 30309	Safety Analysis and Risk Assessment Requirements
SSP 50021	Safety Policy and Requirements
SSP 50021	Safety Policy and Requirements
	ELV Only
NASA-STD-8709.2	NASA Safety and Mission Assurance Roles and Responsibilities for Expendable Launch Vehicle Services
	ELV Payloads
NASA-STD-8719.8	Expendable Launch Vehicle Payload Safety Review Process Standard

3. DEFINITIONS

3.1 Accepted Risk - A hazard whose risk is not completely mitigated and that has been accepted by top program and safety management.

3.2 Assessment - Review or audit process, using predetermined methods, that evaluates hardware, software, procedures, technical and programmatic documents, and the adequacy of their implementation.

3.3 Catastrophic - A hazard that could result in a mishap causing fatal injury to personnel, and/or loss of one or more major elements of the flight vehicle or ground facility.

3.4 Controlled (Risk) Hazard - The likelihood of occurrence or severity of the associated undesirable event has been reduced to an acceptable level through the imposition of appropriate, readily implementable, verifiable controls which results in minimal residual risk.

3.5 Credible Condition (Event) - Condition (event) that reasonably may be anticipated and planned for on the basis of experience with or analysis of a system.

3.6 Critical - A hazard that could result in a mishap causing a non-disabling injury to personnel and/or damage to one or more major elements of the flight vehicle or ground facility.

3.7 Eliminated Hazard - A hazard that has been eliminated by completely removing the hazard causal factors.

3.8 Event Tree Analysis - An analysis that traces the effect of a mishap and leads to all possible consequences through visualization of the positive and negative aspects of each event using a type of logic tree. Event trees are complements to fault trees. This is an inductive logic method for identifying the various possible outcomes of a given initiating event.

3.9 Failure/Fault - Inability of a system, subsystem, component, or part to perform its required function within specified limits.

3.10 Fault Hazard Analysis - Analysis performed during design resulting in the identification, evaluation, and control of hazards resulting from piece-part or component faults.

3.11 Failure Tolerance - Built-in capability of a system to operate in the presence of specified hardware or software failures without the occurrence of a hazard.

3.12 Fault Tree Analysis - An analytical technique whereby an undesired state of the system is specified and the system is then analyzed in the context of its design, environment, and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphical model of the various parallel and sequential combinations of faults that result in the occurrence of the predefined undesired event.

3.13 Hazard - Existing or potential condition that can result in or contribute to a mishap.

3.14 Hazard Analysis - Identification and evaluation of existing and potential hazards and the recommended mitigation for the hazard sources found.

3.15 Hazard Control - Means of reducing the risk of exposure to a hazard.

3.16 Integrated Hazard Analysis - Comprehensive evaluation of hazards, taking into account all subsystems/elements which are included in the overall system being analyzed, including the system's operational and environmental envelopes.

3.17 Interface Hazard Analysis - Evaluation of hazards which cross the interfaces between a specified set of components, elements, or subsystems.

3.18 Noncompliance Report - A formal report documenting a condition in which a requirement cannot be met and the rationale for concluding that the noncompliance condition is safe.

3.19 Operating and Support Hazard Analysis - An analysis performed to identify hazards and recommended risk reduction alternatives in procedurally controlled activities during all phases of intended use.

3.20 Operating Hazard Analysis - An analysis that examines the operator interface during system operation and maintenance activities. The analysis defines certification and training requirements as well as safety inputs to technical manuals, warning signs, and safety placards.

3.21 Preliminary Hazard Analysis - A gross study of the initial system concepts used to identify all the sources that constitute inherent hazards. The sources are examined for possible failures in every mode of system operation and methods for protecting against potential mishaps are identified.

3.22 Risk - Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesired event, the potential severity of the resulting consequences, and the uncertainties associated with the frequency and severity.

3.23 Risk Management - Process of balancing risk with cost, schedule, and other programmatic considerations.

3.24 Safety Analysis - Generic term associated with a family of analyses used to identify and control hazards.

3.25 System Safety - Application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks with the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

3.26 System Safety Program Plan (SSPP) - A document that describes the safety assurance tasks to be implemented throughout a program/project or contract, including methods of approach, safety milestones, and assigned responsibilities for fulfilling these tasks.

4. INSTRUCTIONS

The approach to performing a hazard analysis is a seven step process. The instructions below detail the steps to be followed in the hazard analysis process. The flow diagram given in Section 11 depicts this process graphically.

4.1 **Gather Data.** The system safety analyst shall identify information and data resources pertinent to the system design, configuration, and operation. This activity includes identifying

cognizant personnel through which data/information may be obtained, as well as collecting the actual documentation that details the design, configuration, and operations data. Pertinent information may be contained in design definition documents, performance specifications, flight and ground operations documents, conceptual and/or engineering drawings, schematics, presentation materials, and other programmatic documentation. The system safety analyst shall participate in Technical Interchange Meetings, progress reviews, requirements reviews, design reviews, etc., to obtain significant information. A list of key technical discipline personnel for the project is typically maintained by Project Management and should be used by the System Safety engineer to identify interfaces to the technical disciplines. Questions concerning the system under study or with the documentation being collected shall be directed to these personnel. Other potential sources of useful data can be obtained from previous analyses, tests, or inspections of the same or similar systems as well as from lessons learned or historical databases.

4.2 **Learn the System**. Before the hazard analysis can be initiated, the system design and operation shall be fully understood by the system safety analyst. The analyst shall read and study the data gathered in 4.1 above and ask questions of the key technical personnel as appropriate to aid in understanding the system. In addition to an understanding of the system design and operation, the system safety policies and requirements for that system shall be thoroughly understood (e.g., NSTS 1700.7, NSTS 22254, SSP 50021, etc.) by the system safety analyst.

4.3 **Define the Scope and Type of Analysis**. This step may vary depending on the system to be analyzed and the life cycle phase of the project. The applicable system safety requirements may be mandated through a tailored System Safety Program Plan (SSPP) or in other NASA policy and requirements documents. However, fundamental decisions in defining the scope and type of analysis which are common to all projects include: (1) deciding what to analyze, (2) determining the level of analysis detail, and (3) ensuring the analysis task is focused at a manageable level. Unique project requirements are levied as follows:

a. Space Shuttle. Space Shuttle hazard analysis requirements are detailed in NSTS 22254.

b. Payloads. There are numerous requirements documents for payload hazard analysis depending on the launch/landing vehicle and the vehicle on which payload operations occur. The following matrix provides a summary of the payload safety requirements documents.

Launch Vehicle/ Operation	Space Shuttle	ISS	ELV
Space Shuttle	NSTS 1700.7 KHB 1700.7 NSTS 13830	NSTS 1700.7 NSTS 1700.7, Addendum 1 KHB 1700.7 NSTS 13830	N/A

ELV	N/A	N/A	AFSPCMAN 91-710

NSTS 13830 and EWR 127-1 define the scope and detail required in the analysis. The other documents establish safety policies and technical requirements.

c. Space Station. The hazard analysis scope and detail required for Space Station is defined in SSP 30599 and SSP 30309. The safety policy and technical requirements are defined in SSP 50021.

d. Reusable Launch Vehicle. The current requirements for RLVs are defined in the project SSPP. MIL-STD-882 provides general information regarding the scope of hazard analyses.

4.4 **Select an Analytical Technique**. There are numerous techniques available for performing a hazard analysis. The particular technique used by the system safety analyst may vary from project to project but shall provide the required level of detail based upon project requirements. NPR 8715.3 provides several techniques for consideration. The analytical technique provides the focus and systematic process for performing the analysis.

4.5 **Perform the Analysis**. The analysis shall be completed by the safety analyst using the technique(s) selected in 4.4. This is not the documentation step; however, copious notes taken during this step aid in the documentation process to follow. The emphasis here is on the application of the analytical technique to the system under review.

4.6 **Document the Analysis**. After the analysis is complete, it shall be documented by the analyst according to the specific project requirements.

a. Space Shuttle hazard analysis shall be documented according to the requirements in NSTS 22254.

b. Payload hazard analysis shall be documented according to requirements based on the launch vehicle and the vehicle on which the payload operates (Reference 4.3b)

c. Space Station hazard analysis shall be documented according to the requirements in SSP 30599.

d. RLV hazard analysis shall be documented according to requirements specified in the SSPP.

4.7 **Provide Feedback**. The documented hazard analysis shall be provided by the system safety analyst to project management, engineering design personnel, and review boards/panels as required by the specific project. The results of the hazard analysis and associated data shall be reviewed by the entire project team on a periodic basis (as established by project requirements)

and approved by authorized personnel prior to issue. Changes to previously approved documentation shall be reviewed and approved by the same functions/organizations that performed the original review and approval.

5. NOTES

5.1. This issuance replaces QS10-SS-011C, dated Sept. 9, 2002

6. SAFETY PRECAUTIONS AND WARNING NOTES

None.

7. APPENDICES, DATA, REPORTS, AND FORMS

None.

8. RECORDS

None.

NOTE: The Safety and Mission Assurance Directorate performs hazard analyses at the request of the cognizant MSFC Project Office. As a result, the completed hazard analysis documentation is submitted to the appropriate Project Office and becomes the property of that Office. Therefore, neither the hazard analysis documentation nor any of the data obtained or created through the process described in Section 4 above is maintained by the Safety and Mission Assurance Directorate as a Record.

9. TOOLS, EQUIPMENT, AND MATERIALS

Many computer software packages are available to assist the System Safety engineer in performing the hazard analysis activities described in Section 4. The use of specialized computer software applications is encouraged but shall be approved by the Director of the MSFC Safety and Mission Assurance Directorate. Specialized computer software applications is defined as those software packages not available via the current suite of applications found on the MSFC computer systems network (e.g., DDS).

10. PERSONNEL TRAINING AND CERTIFICATION

Safety and Mission Assurance Directorate personnel involved in hazard analysis activities shall have an engineering or other approved technical background. Training in hazard analysis techniques is not required but is strongly encouraged. Training can be obtained through various courses offered periodically by the MSFC Training Branch. The training program used for

System Safety Engineers at MSFC is documented in the Professional Development Roadmap (PDRM) for System Safety Engineers, document number QD-A-005.

11. FLOW DIAGRAM